“LAS POLITICAS PÚBLICAS DE SEGURIDAD EN LATINOAMÉRICA. CONOCIMIENTO, ANÁLISIS Y PROPUESTAS.”

Curso a cura del Dr. Fernando Gabriel Zarabozo

Sesión Setiembre-Diciembre 2020

Trabajo final a cura del participante al curso: Dino Mora

El concepto de Sistema de Inteligencia Integrado (IIS) en el entorno estratégico de las políticas de seguridad de América Latina. Análisis y propuestas.

RESUMEN EJECUTIVO

El entorno de seguridad global está cambiando rápidamente. El futuro presenta a América Latina oportunidades sin precedentes para influir positivamente en el entorno de seguridad y, al mismo tiempo, garantizar la agilidad y flexibilidad para responder a desafíos impredecibles y complejos. En consecuencia, este breve documento está destinado a inspirar y apoyar el diálogo estratégico sobre los desafíos que América Latina enfrenta y enfrentará y las correspondientes implicaciones militares y de seguridad. No quiere predecir el futuro ni presumir decisiones políticas que determinarán los roles y las capacidades requeridas de los países latinoamericanos. Más bien, le gustaría brindar a los tomadores de decisiones de la región consideraciones adicionales para superar los desafíos planteados por el entorno futuro de la seguridad.

Cambios en el entorno estratégico durante las décadas de 1980 y 1990, un proceso de democratización que puso fin a los gobiernos militares del siglo XX, el incremento de operaciones en temas diferentes de la “guerra tradicional”, que término’ con la fin de la Guerra Fría, dio’ una profunda revolución a la doctrina de seguridad nacional de los países de América Latina.

Estos profundos cambios doctrinales, se manifestaron a la opinión pública latinoamericana y mundial con una traslación de objetivos estratégicos en las políticas de seguridad de los países, donde la cuestión criminal y la seguridad ciudadana se convirtieron en temas centrales de la agenda política.

Esto dio’ lugar a que muchos países favorecieran el involucramiento de los militares en el “combate a la criminalidad” y vio’ la creación del concepto de “nuevas amenazas” (criminalidad organizada transnacional, narcotráfico y terrorismo entre otras) para justificar el utilizo de las Fuerzas Armadas en temas de fuerzas policiales, y convencer las autoridades y la opinión públicas de que no existe una diferencia de naturaleza entre la seguridad ciudadana y la defensa nacional.

Del involucramiento de militares en tareas de seguridad se derivan posibles problemas políticos e institucionales:

- esta política reflecte la desprofesionalización de las Fuerzas Armadas, que han sido entrenadas y equipadas para actividades y operaciones relativas a la defensa nacional y no están capacitadas para resolver de forma eficaz problemas de criminalidad;

- el recurso a las Fuerzas Armadas esconde los problemas estructurales de las fuerzas policiales, tanto en materia de corrupción como de ineficacia, así que no se procede en las reformas estructurales que las policías necesitan y proporcionalmente, se pone en riesgo una posible degradación de la institución militar (por ejemplo, en Guatemala ex miembros de la unidad especial del Ejército conocida como Los Kaibiles fueron reclutados por el cartel mexicano de Los Zetas para transmitirles técnicas y conocimientos específicos adquiridos durante su entrenamiento militar);

- la asignación de misiones de seguridad pública implica una expansión de la presencia militar en el sistema político y en la sociedad y esto podría resultar especialmente riesgoso a causa de una militarización que tiende a otorgar mayores niveles de autonomía a las fuerzas militares, a desequilibrar las relaciones cívico-militares y, en consecuencia, a reducir la conducción política del poder civil (por ejemplo, lo que paso' con la política de "la mano dura" en Brasil).

(fuente CELS)

Estas transformaciones institucionales y de políticas en la seguridad y la defensa, interesaron todos los sectores y niveles de las estructuras de las Fuerzas Armadas y de las Fuerzas Policiales y todas las capacidades que ellas podían producir y desarrollar, incluida la inteligencia y el proceso informativo, que a frente de los nuevos retos, demostró una insuficiencia en la arquitectura de inteligencia testimoniada da claras e registrada ineficiencias en las capacidades de recolecciones, análisis y producciones informativas, lo que requiere una revisión de esta importantísima capacidad.

Todo esto, no significa que las fuerzas armadas no puedan "suportar" las fuerzas policiales en tareas de ordine público y seguridad ciudadana, con los débitos presupuestos y requisitos de coordinación y comando. Por ejemplo en Italia desde casi 20 años existe una operación nacional conjunta llamada Operación "Strade Sicure" (Calles Seguras) donde el Ejército, con rotaciones de 6 meses, ofrece unidades a nivel de Task Force "Fuerzas Conjuntas" (nivel de regimiento reforzado con unidades de reservas y otros suportes) a las fuerzas públicas italiana. Se destacan pequeñas unidades de 3-4 soldados con equipo individual en suporto a los Carabinieri y Polizia por el control de puntos estratégicos de las grande ciudades: parcos turísticos, plazas grandes, monumentos, calles principales ecc…con la tarea de primera intervención en flagrancia e suporte a las actividades de seguridad pública y defensa de la ciudadanía, típicas de las fuerzas policiales. Las unidades del Ejército, constitucionalmente, son entrenadas en actividades de ordine públicos (antimotines, control vial, detención y arrestos, puntos de control, ecc…) en razón de las actividades que desempeñan en las operaciones multinacionales de la OTAN y por esto es bueno para ellos participar a esta operación nacional porque resulta ser una buena ocasión para "entrenar como combate", como se dice, ósea entrenar en un entorno prácticamente real, que es lo de la seguridad ciudadana del país.

De particular relevancia, este suporte hubo un gran éxito en el sur de Italia en el combate de la mafia y el control de los tráficos ilegales. Además desde Marzo 2020, las unidades del ejército empeñadas en la operación, desempeñaron un gran suporte a las fuerzas públicas en el control de las restricciones y los movimientos debidos al Covid 19, que en Italia fueron, y están siendo, muy duras. Conjuntamente a las

patrullas de Polizia y Carabinieri, participaban a los puntos de control en toda Italia para ayudarlos y garantizar la seguridad de los ciudadanos.

Esta actividad de suporte y colaboración de las diversas fuerzas nacionales, fue' posible gracias a acuerdos entre los comandos estratégicos y los diferentes Ministerios para establecer el OPCOM (Comando operativo) y OPCON (Control operativo) de las unidades del Ejército en coordinación con las fuerzas públicas, y el establecimiento de un centro operativo estratégico donde representantes de los comandos de las fuerzas armadas empeñada en la operación, coordinan las actividades con los comandos territoriales, regionales y nacionales de las fuerzas públicas, juntos en un único comando nacional combinado.

Entre las actividades que beneficiaron de esta organización combinada y conjunta, se encuentra una mayor difusión de las informaciones y la función de inteligencia tuvo un gran éxito porque fueron puestos a trabajar en la misma tarea, con el mismo objetivo, bajo un único comando combinado, diferentes tipos de activos, de operadores, con diferentes tipos de capacitaciones, entrenamientos y conocimientos. La operación continúa hasta el día de hoy con mucho éxito, desde casi 20 años.

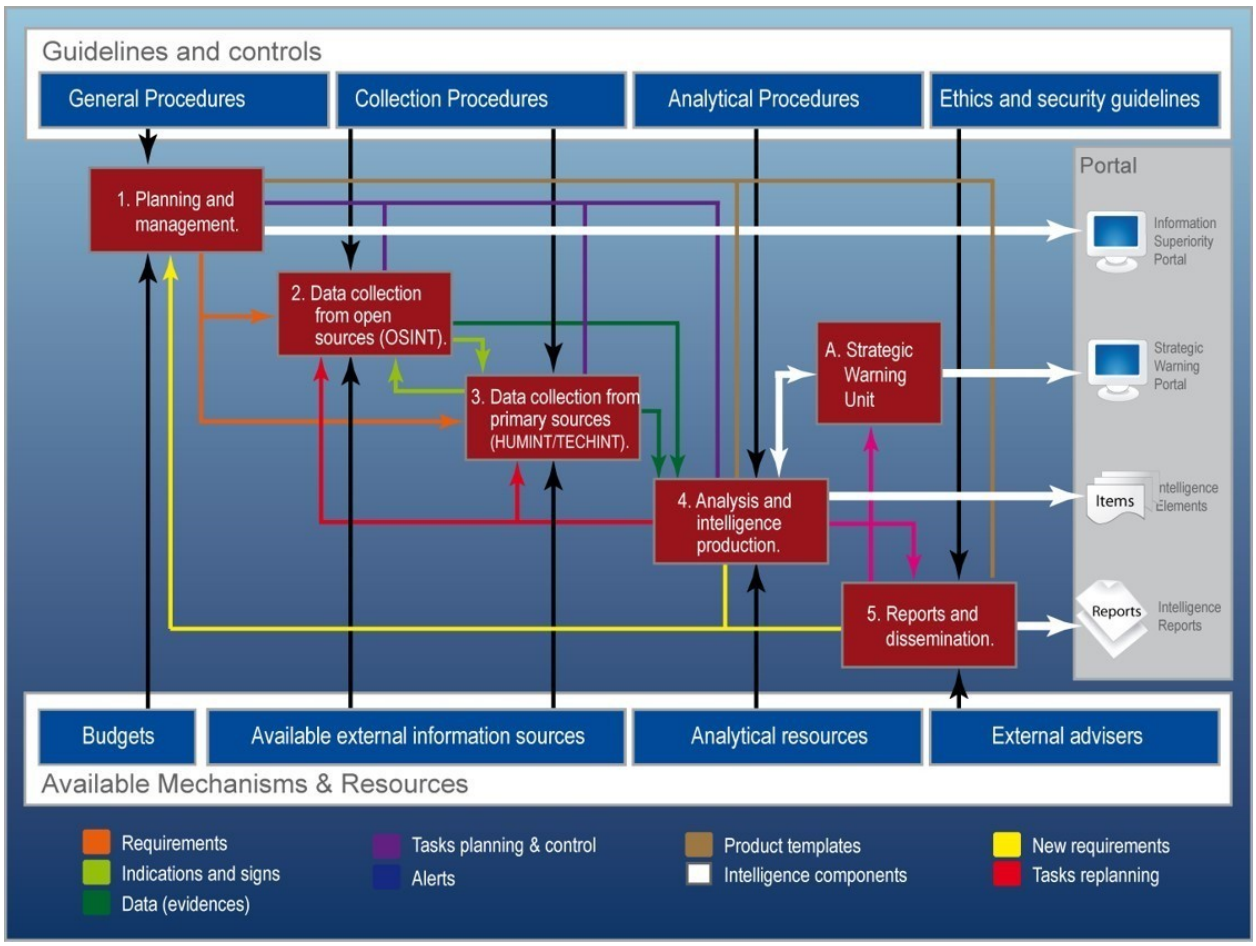
El objetivo deseado de este papel es la revisión de las insuficiencias de los procesos de inteligencia y la manifestación de sugerencias para el incremento de esta función, en una visión regional y integrada, entre los países integrantes de América Latina.

Entre los 80 y 90, América Latina fue interesada en nuevas misiones y las capacidades se debieron lentamente adaptar a las nuevas realidades. En algunas áreas los progresos fueron más lentos y la eficiencia operativa sufrió de este atraso. Una de estas áreas fue' la inteligencia, y principalmente se evidencio' una falta total de un sistema de inteligencia y así' mismo, la ausencia de una comunidad de inteligencia. No de un solo país, si no una realidad y una necesidad de toda la región.

Hoy, las capacidades de inteligencia de los países de América Latina, son capacitadas, flexibles y de inmediata efectividad pero' presentan dificultades en desarrollar un sistema de trabajo idóneo para suportar las operaciones enfocadas al combate del terrorismo, o a las operaciones de crisis dinámicas que las "nuevas amenazas" proponen día a día. Y el resultado, lo vemos en frente de nosotros, lo vivimos directamente en el cotidiano, porque la violencia, el crimen, la corrupción y las "nuevas amenazas", en vez de disminuir, aumentaron exponencialmente en los últimos anos.

Algo no funciona bien.

Las lecciones aprendidas en las recientes operaciones indican que a despecho de la existencia de capacidades nacionales, los tomadores de decisiones, los equipos operacionales y las fuerzas tácticas, les faltan las informaciones cruciales que necesitan para entender el ambiente operativo donde deben operar y decidir. La razón es que planificar, asignar tareas y explotar los instrumentos de la inteligencia, los sensores, los activos y las actividades, de todos los países involucrados en esta batalla, es lento, aislado e ineficiente. Por eso, hay una urgencia en examinar los requisitos de un sistema de inteligencia conjunto y combinado para América Latina.



Módulo de Sistema de análisis de inteligencia ASAS (All Source Analysis System)

DEFICIENCIAS y PROPUESTAS

En el estudio y análisis de diferentes operaciones en países como Brasil, Guatemala, México, se identificaron algunas deficiencias principales en los procesos de inteligencia nacionales, que actúan de obstáculo a la creación de un sistema de inteligencia integrado:

- los sistemas nacionales actuales no pueden satisfacer los requisitos de información globales necesarios, principalmente debido al hecho de que sus sistemas, arquitecturas y procesos fueron diseñados para un entorno operativo muy diferente, regional, compartimentado y no fueron actualizados;

- carecen del número requerido y de la combinación de capacidades de recolección. Los activos integrados son pocos y, en general, propiedad de estados que no siempre están dispuestos a asignarlos a otros estados. Algunos también tienen una capacidad limitada;

- carecen de coherencia y cooperación entre organizaciones. Los comandos, el personal y los individuos no han sido capacitados ni equipados para operar en un entorno que federe diversas capacidades en todos los niveles, militar (estratégico a táctico) y civil, conectados a través de una infraestructura de información tecnológica (IT) común y compartida, donde la información se comparte y las tareas se realizan a través de fronteras. En consecuencia, gran parte de estas actividades de inteligencia todavía se llevan a cabo en forma compartimentada;

- no pueden acceder o compartir inteligencia e informaciones con otros elementos de otras naciones, socios y actores no tradicionales en el teatro de la misma operación por razones técnicas, procedimentales y culturales.

Para resolver estas deficiencias, se pueden individuar algunos principios da implementar:

- el suporte combinado y conjunto de las estructuras nacionales de defensa y seguridad a la totalidad de los espectros de las operaciones. Los países de la región deben poder operar en todo el espectro de los conflictos y "nuevas amenazas" y las capacidades de inteligencia combinadas deben adaptarse a este concepto, utilizando los principios de un enfoque integral;

- el sistema de inteligencia integrado consiste en los números correctos y la combinación de medios de recolección en acuerdo con las tareas operativas. Los actores estatales requieren acceso a, o propiedad de, activos de recolección de inteligencia integrados, adecuados para lograr sus tareas. Se acepta que nunca habrá suficiente, de ahí que se requieran procedimientos dinámicos de gestión de las informaciones y asignación objetivas de tareas, que maximicen los avances tecnológicos para lograr los efectos deseados;

- las actividades del sistema de inteligencia integrado son combinadas y en consecuencia más eficientes y efectivas que las operaciones de un único servicio de inteligencia o de las operaciones de una sola agencia de inteligencia. Durante mucho tiempo se ha aceptado que operar como una fuerza conjunta optimiza la efectividad de las contribuciones a las operaciones más que un solo servicio. El mismo principio sirve por la efectividad del sistema de inteligencia integrado. El concepto busca maximizar los beneficios de la unión en el campo de las operaciones de inteligencia combinadas y rendir el producto de inteligencia "accionable": eficaz, lo más cercano a la realidad y inmediato.

- El sistema de inteligencia integrado debe ser habilitado en una red informática común y suportado da un Collection Coordination Intelligence Requirements Management (CCIRM) y da procedimientos de gestión de las informaciones. Todas las operaciones serán gestionadas en una infraestructura de información tecnológica (IT) común a todos los países integrantes, donde las arquitecturas de inteligencia serán orientada al desarrollo de las tareas tácticas, operacionales y estratégicas, que permitirá a los comandos y a los operadores de acceder a la inteligencia compartida entre todos, a través de la provisión de productos de inteligencia directamente en la red informática. El IIS será estructurado en una serie de servicios y actividades que permitirán a los comandantes, a los estados mayores, a los operadores y a los analistas de tener la justa información, al momento justo y en el lugar justo. Como se puede obtener este resultado?

Creando una actividad de inteligencia que integra y sincroniza la adquisición, planificación y procedimientos de todos los activos de recolección con las funciones de procesamiento, explotación, fusión y difusión en apoyo directo a los tomadores de decisiones en todos los niveles de mando.

La implementación de este proyecto debería ser asignada a un grupo de trabajo integrado de desarrollo de capacidades, con miembros de los servicios de inteligencias de los países latinoamericanos que representarán la misma comunidad de inteligencia, sus gobiernos, sus comandos nacionales y agencias. Los miembros de este grupo de trabajo coordinan los esfuerzos para presentar el programa de desarrollo del sistema de inteligencia conjunto, una visión de lo que será el sistema y los pasos para su implementación, que ira' en paralelo con la implementación del ciclo de inteligencia actual, no más atinente al análisis de las nuevas amenazas y a los nuevos retos, así que se explotaran los desarrollos futuros y los requisitos por realizar este proyecto regional.

El SISTEMA DE INTELIGENCIA INTEGRADO (IIS).

Definición del sistema. "Es una actividad basada en inteligencia operativa que integra y sincroniza la adquisición, planificación y operación de todos los activos de recolección con las funciones de procesamiento, explotación, fusión y difusión en apoyo directo de los responsables de la toma de decisiones en todos los niveles de mando ".

La comunidad de inteligencia. Los Comandos, organizaciones, organismos y agencias en la región y las naciones que desempeñan estas funciones y actividades componen la comunidad del SISTEMA INTEGRADO DE INTELIGENCIA.

Implícito en la definición. Los siguientes aspectos del sistema integrado no se establecen específicamente en la definición, pero se consideran implícitos por las siguientes razones:

(1) El espacio-misión del IIS contiene tierra, mar, submarino, aire y el espacio sobre ellos, objetos naturales y artificiales, y el espectro electromagnético y el ciberespacio. El IIS es una actividad realizada por sensores conectados a sistemas analíticos y de explotación e incluye humanos y plataformas que recolectan y explotan información en todos los dominios, operados por fuerzas aéreas, terrestres marítimas, de operaciones especiales, así como fuerzas policiales y agencias militares. Los sensores IIS pueden ser estáticos o móviles, transportados en satélites, aviones, vehículos terrestres, barcos y personas, incluidos ojos, oídos y otros sentidos humanos. Los fenómenos y fuentes detectados para IIS incluyen, entre otros, luz, calor, radar y otras ondas electromagnéticas (activas o pasivas), sonido, vibración y partículas, en forma de imágenes, firmas, actividad humana, documentos y multimedia, información casi en tiempo real y archivada, incluida información de fuentes abiertas. Los datos producidos o recopilados pueden difundirse casi en tiempo real a los usuarios.

(2) Las diferentes comunidades tradicionalmente ponen mayor énfasis en la inteligencia, la vigilancia o el reconocimiento en función de sus capacidades y propósitos orgánicos. La información recopilada a través de todas estas actividades apoya directamente muchos usos, incluidos el

conocimiento de la situación (SA) de los comandantes, la advertencia de amenazas y la adquisición de objetivos (TA). Por estas razones, son comunes diferentes permutaciones del nombre dado a estas actividades (por ejemplo, Adquisición de objetivos de vigilancia de reconocimiento (RSTA), Adquisición y reconocimiento de objetivos de vigilancia de inteligencia (ISTAR) y otras variantes). En este concepto, el término IIS se utiliza en el entendimiento de que la información recopilada respaldaría los requisitos de toma de decisiones en todos los niveles de mando y, por lo tanto, incluir áreas específicas como la focalización o el conocimiento de la situación sería redundante. El requisito de la información recopilada debe entenderse como cliente de IIS.

(3) La palabra "integrada" asume una importancia particular en la definición de Sistema de Inteligencia, para enfatizar los beneficios y la importancia de la articulación para mejorar la interoperabilidad entre los componentes, las fuerzas orientadas al servicio único, sus equipos y otras organizaciones.

Deficiencias identificadas de los sistemas de inteligencia nacionales

Deficiencias y carencias. Desde principios de la década de 1990, América Latina ha estado involucrada en una serie de operaciones de respuesta a crisis para las cuales las diferentes capacidades de inteligencia nacionales no fueron diseñadas o desarrolladas originalmente. Apuntar a Venezuela, encontrar fuerzas irregulares en Colombia, identificar puntos conflictivos sociales y culturales, amenazas urbanas y apoyar el socorro en casos de desastre en montañas y selvas remotas, han requerido, pero no logrado por completo, la recopilación y entrega de la inteligencia oportuna que necesitan los operadores, planificadores y tomadores de decisiones. Las siguientes son solo algunas de las deficiencias más críticas:

a) Incapaz de satisfacer los requisitos de información. Los activos, procesos y políticas de inteligencia actuales no están diseñados para los requisitos operativos actuales y son inadecuados.

1) Inteligencia oportuna. La asignación de las actividades de inteligencia y el intercambio de la información de inteligencia más dinámica generalmente no es posible en LATAM por una variedad de razones (política nacional, activos y capacidades limitados, cultura, etc.). Las naciones generalmente solo comparten información filtrada en forma de productos terminados. Por lo tanto, la falta de información dinámica y el intercambio de datos impide que la infraestructura de inteligencia nacional y el personal de operaciones produzcan productos operativos e inteligencia de manera oportuna.

2) Necesidad de construir el Cuadro Operativo Común (COP). Actualmente, la mayor parte de la información de inteligencia nacional no se transfiere al cuadro operativo común de la región. Los sistemas existentes que muestran imágenes terrestres, aéreas y marítimas reconocidas se limitan a muy pocas fuentes de datos y no satisfacen las necesidades de las fuerzas operativas y tácticas.

3) Inteligencia no tradicional. Las técnicas actuales de análisis de inteligencia se centran en el apoyo tradicional a las operaciones de combate. La lucha contra el terrorismo, la contrainsurgencia, la guerra urbana, la asistencia humanitaria, la estabilización y la

reconstrucción presentan desafíos únicos para las capacidades del IIS diseñadas para las operaciones tradicionales de aplicación de la ley. Es necesario realizar esfuerzos para desarrollar y capacitar las habilidades, técnicas y fuentes necesarias para cumplir con estos requisitos.

b) Falta de capacidades. A pesar de los desarrollos recientes, muchas naciones de LATAM solo tienen capacidades de inteligencia limitadas y ciertamente no lo suficiente para satisfacer demandas altas o concurrentes. Por estas y otras razones, las naciones no comprometen sus activos limitados a misiones comunes, lo que genera algunos de los siguientes problemas:

   1) Falta de activos comunes. Los comandantes en todos los escalones no tienen activos bajo OPCON (Control Operativo) o propios para la tarea y solo un número limitado ofrecido por otras naciones para tratar de coordinarlos. Dependen de productos nacionales y agencias de inteligencia nacionales como vehículo de información. Ninguno de estos es tan eficiente y oportuno como tener capacidades orgánicas. Por ejemplo, no existe un Sistema de Defensa Aérea integrado que brinde vigilancia, reconocimiento, una imagen aérea reconocida y funciones de control aéreo a los comandantes operativos aéreos y marítimos, y esta es solo una capacidad en un espectro de capacidades requeridas necesarias para lograr la visión IIS.

   2) Sin redundancia. Nunca hay suficientes activos para garantizar la redundancia y los medios son limitados para la señalización cruzada y la corroboración de la detección de una sola fuente. Los activos de inteligencia suelen tener una capacidad limitada y no son adecuados para la amenaza o el entorno operativo. Por lo tanto, no hay redundancia para "no recopilar" al planificar el uso de información de una misión en particular. El cliente simplemente se queda sin, independientemente de la importancia de la misión, ya que rara vez hay medios para asignar otra capacidad para recopilar, en un sentido dinámico, en el área de interés omitida.

   3) Capacidad de sensor limitada. Se requiere una amplia gama de sensores para analizar entornos operativos en sus espectros completos (por ejemplo, terrenos urbanos). Estos requieren sensores que detecten fuera del espectro visible óptico e infrarrojo estándar. Estos sensores incluirían sistemas que cubren diferentes partes del espectro electromagnético, incluidos sensores multiespectrales e hiperespectrales. En el entorno terrestre, por ejemplo, también pueden ser necesarias otras clases de sensores, incluidos sensores sísmicos y acústicos.

c) Falta de coherencia y cooperación entre organizaciones. Siempre ha habido dificultades para integrar las capacidades y actividades de diferentes organizaciones, agencias de aplicación de la ley y departamentos. Las razones de esto incluyen diferentes objetivos, misiones, terminología, cultura y sistemas, con los problemas resultantes que ocurren:

1) Limitaciones organizativas. Los requisitos de información conjuntos de los comandantes, los componentes y las fuerzas terrestres, aéreas, marítimas y de operaciones especiales a menudo se consideran dentro de sus propias estructuras organizativas. Asimismo, los recursos de inteligencia de las fuerzas terrestres, aéreas, marítimas y de operaciones especiales a menudo se emplean de la misma manera sin cumplir con los requisitos de prioridad dentro de la fuerza conjunta e integrada. Las capacidades de IIS terrestres y marítimas a menudo se descuidan en un proceso de recolección centrado en el aire e incluso los activos aéreos que pertenecen a componentes terrestres y marítimos a menudo se limitan a funciones de apoyo a la misión en lugar de activos de recolección.

2) Limitaciones de los comandantes. El comando y control (C2) de las actividades de inteligencia no está coordinado a través de la fuerza conjunta. Con frecuencia, los comandantes no están al tanto de las operaciones de recolección en su área de interés y no pueden resolver los conflictos según sea necesario. La capacidad de reasignar dinámicamente los activos de recopilación en apoyo de operaciones urgentes no es posible excepto dentro de un solo componente. Hay razones culturales y físicas por las que los planificadores y administradores de recolecciones no pueden y, por lo tanto, no colaboran activamente en la coordinación de requisitos y activos. En cambio, tienden a depender del proceso de RFI (Solicitud de Información) más lento. Incluso dentro de comandos únicos, los elementos del personal de inteligencia, operaciones y comunicaciones con frecuencia no trabajan juntos para maximizar las capacidades y requisitos de IIS.

3) El entrenamiento de inteligencia es actualmente demasiado artificial, si no existe. La práctica de la inteligencia durante los ejercicios combinados es demasiado artificial o inexistente y no prepara al personal y las fuerzas para los desafíos que enfrentan en las operaciones reales.

d) La información no es accesible ni compartida. Debido a la falta de capacidades habilitadas para la red y aplicaciones militares y de aplicación de la ley, la mayoría de los recolectores de inteligencia y su información permanecen almacenados en bases de datos aisladas, sistemas y redes limitadas. Los problemas relacionados con esta falta de conectividad y acceso incluyen:

1) Las personas y organizaciones que realizan funciones de inteligencia no utilizan sistemas y redes interoperables. Además, sus aplicaciones no son interoperables.

2) Los sensores se utilizan a menudo solo para funciones específicas, como investigaciones, mientras que podrían integrarse y ser útiles para otras fuerzas y departamentos. Los datos y la información procesada que proviene de muchos sensores y actividades de recolección no están directamente conectados ni son interoperables con las herramientas y sistemas utilizados para el comando y control y la gestión de seguridad, planificación operativa, explotación u otros servicios funcionales. Esto significa que la información no llega a quienes la necesitan de manera oportuna y en una forma que puedan usar.

3) La mayoría de las naciones que proporcionan activos de recopilación conectarán o entregarán los datos recopilados a una estación o instalación terrestre nacional donde se procesan y

explotan en los sistemas y redes nacionales antes de que se pasen a otras naciones (usuarios) y niveles. El resultado es que la información llega tarde, si es que llega todo. La distribución en tiempo real de datos de múltiples sensores requiere una red que tenga suficiente ancho de banda para permitir la transferencia de grandes volúmenes de datos y la capacidad de ingerir datos de una amplia gama de capacidades de recopilación nacional.

4) No existen procesos de gestión de la información para garantizar que la información relevante llegue al lugar correcto en el momento correcto en el formato más útil. Cuando la información no comienza a fluir hacia los usuarios, puede causar un bloque en el flujo informativo y una sobrecarga de información que es deletérea para una tarea determinada.

Visión de un sistema de inteligencia integrado

Principios. Para abordar las principales deficiencias discutidas en la sección anterior, cuatro principios generales son fundamentales para lograr la visión de un sistema de inteligencia integrado. El mando y control, los procesos de planificación y la interoperabilidad están implícitos o están estrechamente relacionados con estos cuatro principios. Por esta razón, los cuatro principios sirven como un medio para categorizar los requisitos de capacidad y el desarrollo en este concepto. Estos principios de IIS no están destinados de ninguna manera a reemplazar otros principios operativos o atributos de los procesos de inteligencia. Los cuatro principios son:

- **IIS admite todo el espectro de operaciones de inteligencia**. - Las capacidades y actividades de IIS deben satisfacer los requisitos de información de planificación, ejecución y evaluación de los encargados de la toma de decisiones políticas, los comandantes estratégicos, operacionales y tácticos, el estado mayor y las fuerzas de las naciones en cada fase de las operaciones. El espectro completo (o continuo) de operaciones se extiende desde las amenazas tradicionales, las "nuevas amenazas", hasta el apoyo a la paz, las operaciones humanitarias y de evacuación, así como las operaciones de estabilización y reconstrucción.

- **IIS consta de los números correctos y la combinación de medios de recopilación en acuerdo con la tarea operativa**. Como la mayoría de las capacidades nacionales, IIS es la suma de lo que las naciones se comprometen y contribuyen a misiones específicas, lo que poseen las naciones y los servicios o información adquiridos comercialmente. Los requisitos de las posibles misiones de espectro completo exigen una amplia gama de capacidades de IIS, muchas de las cuales son identificadas por los comandantes operativos y mediante el Proceso de planificación de defensa. Este principio tiene dos aspectos: calidad y cantidad, los cuales son necesarios para garantizar la cobertura de ISR generalizada, persistente y adecuada necesaria para recopilar la información requerida. En general, tener la combinación y el número correctos de activos de IIS proporciona al comandante operativo la agilidad para responder de manera eficaz a muchas situaciones diferentes y mutables.

- **Las actividades de IIS son "conjuntas" y, por lo tanto, más eficientes y efectivas que las actividades de un solo servicio o agencias aisladas**. Volverse más conjunto ha sido uno de los

principios transformadores clave para muchas de las fuerzas armadas y agencias y organizaciones policiales del mundo durante las últimas dos décadas. Los componentes y servicios pueden operar juntos para una mayor efectividad y eficiencia integrando capacidades (incluido IIS), planificación y comando y control, mientras se eliminan las duplicaciones.

- **Las capacidades de IIS están habilitadas en red y respaldadas por la Gestión de requisitos de inteligencia de coordinación de recolecciones (CCIRM) y los procedimientos de gestión de la información**. Por supuesto, el C2 de IIS debe integrarse con otras funciones operativas para garantizar que las mejores capacidades de recopilación disponibles se asignen dinámicamente para respaldar la maniobra, la focalización, el conocimiento de la situación y las evaluaciones. Una vez más, la colaboración en tiempo real es la clave para los procesos C2 que están descentralizados y se adaptan a situaciones que evolucionan rápidamente. Los administradores de recolecciones (para la organización) y los administradores de IIS (para activos específicos) utilizan herramientas de apoyo y comunicaciones para monitorear la ubicación, el estado y la disponibilidad de los activos de IIS, en estrecha coordinación con otros gerentes de los "espacios de batalla". Con la autoridad delegada adecuada, es posible volver a priorizar los requisitos y reasignar los activos y se puede coordinar en tiempo real. C2 se refiere a la autoridad y los arreglos efectivos para realizar operaciones. El tema nunca debe limitarse a los sistemas, pero los procesos de IIS y C2 deben estar respaldados por herramientas de gestión de recolecciones que integren la gestión de la información, la planificación, las operaciones y los procesos de inteligencia. Deben ayudar a los administradores de la gestión informativa con el ciclo de inteligencia en cada fase, desde el requerimiento de información inicial hasta la entrega de esa información al cliente. Entonces, el IIS debe integrarse con otras funciones y sus sistemas. Esto se logra a través de las comunicaciones de red, el intercambio de información y la interoperabilidad que respaldan a IIS y sus clientes.

  El concepto de capacidades habilitadas para la red y los flujos de trabajo asociados buscan evolucionar las capacidades de los sistemas integrados de comando, comunicaciones e información (CCIS) a una federación interoperable y sólida de servicios que se comunican en un entorno en red. IIS debe aprovechar todos los desarrollos relevantes en el concepto de capacidades habilitadas por red (incluida la gestión de datos, información y conocimiento) para hacer el mejor uso de la conectividad, la información archivada y en tiempo real, las aplicaciones y los servicios.

IIS y el ciclo de inteligencia

El funcionamiento de IIS se puede definir en términos de un ciclo que consta de varias fases. La aplicación de los cuatro principios mencionados anteriormente, a la implementación del ciclo de inteligencia y sus fases, es la clave para la transformación de IIS. La planificación, seguimiento y gestión de las actividades en cada fase es necesaria para contar con recursos y apoyo donde y cuando más se necesitan. Del mismo

modo, mientras que la fase de difusión implica llevar la información de IIS al cliente, las herramientas y procesos comunes de gestión de la información y el conocimiento se integran en cada fase. A continuación se describen las fases del mismo:

a) **Definición de requisitos y CCIRM**. En esta fase, los requisitos de información del usuario de IIS se definen, priorizan y consolidan, se dan a conocer a los planificadores y administradores de recolecciones y se realiza un seguimiento de su estado para garantizar que se cumplan. Por lo tanto, la actividad en esta fase incluye la Gestión de Requisitos de Información (IRM), validar los requisitos de información comprobando si la información ya existe en las fuentes de información y bases de datos disponibles (o Base de Conocimiento). La gestión y planificación de la recopilación convierte los requisitos de inteligencia e información de los usuarios de IIS en requisitos de recopilación, formula planes para recopilar información mediante las capacidades de recopilación disponibles y realiza tareas o coordina solicitudes con las fuentes o agencias de recopilación adecuadas, monitorea los resultados y vuelve a realizar las tareas según sea necesario. Además, planifica la comunicación y difusión de la información recopilada según corresponda para garantizar que se cumplan los requisitos de puntualidad. La gestión y planificación de la colección debe ser receptiva y flexible para hacer frente a la naturaleza dinámica de los diferentes requisitos de los usuarios de IIS y las prioridades operativas.

b) **Ejecución de recopilación**. La recopilación se lleva a cabo de acuerdo con el plan de recopilación y sus tareas asociadas (y reasignación de tareas), y la información de recopilación se comunica y difunde según sea necesario.

c) **Procesamiento, Explotación y Fusión**. El procesamiento y la fusión se realizarán según corresponda para generar los productos requeridos por los usuarios de IIS. A través del procesamiento, la información se convertirá en inteligencia o información de nivel superior mediante la recopilación, evaluación, análisis, integración e interpretación. Mediante la fusión, la inteligencia y / o la información de múltiples fuentes o agencias se combinarán en una imagen coherente, donde el origen de elementos individuales ya no es evidente. A través de la explotación, se aprovecharán al máximo los productos que se hayan generado por procesamiento y fusión. La explotación puede realizarse como parte de IIS o por los usuarios de IIS después de la difusión.

d) **Difusión**. La difusión es la transmisión oportuna de información e inteligencia, en una forma apropiada, a los usuarios. La información se puede difundir a los usuarios desde agencias relacionadas con el procesamiento y la fusión o, cuando sea necesario, directamente desde las fuentes de recolección y casi en tiempo real (por ejemplo conectividad entre el sensor y el analista en el centro de fusión) evitando así cualquier procesamiento formal o fusión.

IIS federado. Durante las operaciones, las naciones involucradas en el IIS deberán cumplir con los requisitos de información e inteligencia de una amplia variedad de usuarios del IIS. Estos requisitos variarán notablemente en términos de detalle, alcance y puntualidad, según lo dicte la naturaleza y el ritmo de las operaciones. Estos requisitos no se pueden cumplir con un proceso IIS que presenta una

implementación centralizada de todos los aspectos del ciclo de inteligencia descrito anteriormente. Para proporcionar la capacidad de respuesta necesaria, IIS debe presentar un nivel apropiado de descentralización con capacidades diseñadas para apoyar a comunidades particulares. Estas capacidades deben poder brindar soporte a otras comunidades y, en consecuencia, poder operar juntas de manera federada para crear una capacidad de IIS general. El intercambio oportuno y el intercambio de requisitos, información e inteligencia involucrarán capacidades habilitadas por la red con empresas apropiadas dentro de la federación que serán designadas como fuentes autorizadas de inteligencia e información para aspectos particulares de la misión.

Requisitos de capacidad derivados del concepto.

Requisitos de capacidad.

a) IIS debe satisfacer los requisitos de información de los operadores, planificadores y tomadores de decisiones, tales como que puedan planificar, comandar, coordinar, ejecutar y evaluar el espectro completo de operaciones actuales y futuras.

b) IIS debe apoyar operaciones convencionales, operaciones de evacuación, respuesta humanitaria, respuesta a crisis, antiterrorismo, operaciones de embargo, fuerza de entrada inicial y fuerza demostrativa, junto con tareas de protección de la fuerza. También debe ser compatible con operaciones que requieren una comprensión de los factores del entorno operativo no tradicionales, así como operaciones de seguridad ciudadana.

c) La información recopilada debe ser oportuna, precisa y entregada de la manera y el formato que sea más útil para los clientes. Los datos IIS, las fuentes de los mismos y las interface nacionales a la red compartida deben diseñarse para ser interoperables mediante la adhesión a los STANAG, OPORDER y MOU pertinentes.

d) La comunidad IIS debe ser capaz de planificar, administrar, ejecutar misiones de recolección, reprogramar dinámicamente las tareas según sea necesario, procesar, analizar, explotar, producir y entregar la información requerida por el cliente, en la forma y formato que mejor se adapte al requerimiento.

e) El IIS eficaz debe realizarse utilizando capacidades en red y procesos de colaboración. Estos necesitarán una amplia gama de fuentes, sensores, plataformas, procesos, habilidades, conectividad, herramientas e interoperabilidad. Es necesaria una cantidad y calidad adecuadas de sensores IIS, así como mecanismos de soporte, para permitir la persistencia, el cruce y la recolección en entornos adversos.

f) Deben existir políticas para garantizar la seguridad y el intercambio de la información, y las prácticas efectivas de gestión de la información harán que la información relevante esté disponible mientras se evita la sobrecarga y las duplicaciones.

CONSIDERACIONES FINALES

El enfoque de este concepto debería analizar las debilidades y aportar propuestas para desarrollar e implementar un sistema de inteligencia integrado, conjunto y combinado. Su concepto inicial, deberá ser redactado da un grupo de trabajo especializado que al mismo tiempo representará la comunidad de inteligencia de América Latina, cuerpo doctrinal, formativo y decisional que al momento, representa una falta en el entorno de la inteligencia estratégica de la región.

La comunidad de inteligencia, como cuerpo doctrinal, formativo y decisional y que operaran y implementaran este sistema, debería incluir a los tomadores de decisiones a todos los niveles, los operadores, los desarrolladores de capacidades, los managers y los entrenadores de los comandos y agencias de inteligencia de los países participantes. El concepto desarrollado da el grupo de trabajo dará las direcciones para el desarrollo de las capacidades y las aplicaciones de estas.

Este concepto tiene como tarea la de enderezar los esfuerzos de los piases en satisfacer los requisitos informativos militares y civiles a través de un insume de sistemas y metodologías de inteligencia conjunto y combinado, con metodologías de recolección que utilizan varias fuentes y diferentes disciplinas para realizar un producto de inteligencia que aporte la justa información, al momento justo y en el lugar justo.

Debe Identificar y describir lo que es necesario para proveer una información inmediata, precisa y relevante para los tomadores de decisiones políticas, comandantes operativos, planificadores y fuerzas involucradas en el contexto operativo y táctico. Así como describir como los procesos, las capacidades, las relaciones organizativas y la conectividad deben ser desarrolladas, implementadas y integradas y deberá

enderezar la comunidad de inteligencia de América Latina a trabajar junta y de manera coherente para realizar esta importantísima tarea.